ELSEVIER

Journal of Pure and Applied Algebra 106 (1996) 233–262

JOURNAL OF PURE AND APPLIED ALGEBRA

Multiplicative groups of fields modulo products of subfields

J.-L. Colliot-Thélène [a], R.M. Guralnick[b,*,1], R. Wiegand[c,1]

[a] *Mathématiques, Bât. 425, CNRS, Université de Paris-Sud, F-91405 Orsay, France*

[b] *Department of Mathematics, University of Southern California, Los Angeles, CA 90089-1113, USA*

[c] *Department of Mathematics, University of Nebraska, Lincoln, NE 68588-0323, USA*

Communicated by C.A. Weibel; received 16 December 1993; revised 12 August 1994

Abstract

Let $E_i, 1 \leq i \leq r$, be intermediate fields of the finite separable field extension K/k. We study the quotient $K^*/E_1^* \cdots E_r^*$. We show that there is a dichotomy between the cases $r \leq 2$ and $r > 2$. If $r \leq 2$, then the n-torsion subgroup of that quotient is finite for all $n > 0$, and under suitable hypotheses the entire torsion subgroup is finite. For $r > 2$, examples are given to show that the group $K^*/E_1^* \cdots E_r^*$ may be trivial, finite and nontrivial, infinite torsion or may have infinite torsionfree rank. The case $r = 2$ had been considered earlier in connection with the study of Picard groups of certain singular curves. In the present paper, we study the problem in the more general context of a finite group acting on a module, and then use Galois cohomology.

1. Introduction

Let k be a field and K a proper finite separable field extension of k. Consider the quotient K^*/k^* of the multiplicative group K^* of K by the multiplicative group k^* of k. It is an easy exercise (see Section 4) to show that for any positive integer n, the n-torsion subgroup (set of elements killed by n) of K^*/k^* is a finite group. Also, if k is finitely generated over the prime field, classical results in arithmetical algebraic geometry imply that the whole torsion subgroup of K^*/k^* is a finite group.

Let now E_i $(i = 1, \ldots, r)$ be fields with $k \subset E_i \subset K$. Let $K^*/E_1^* \cdots E_r^*$ be the quotient of the multiplicative group K^* of K by the subgroup spanned by the multiplicative groups E_i^*. For $r \geq 2$, are there finiteness results similar to those mentioned above for $r = 1$?

* Corresponding author. E-mail: guralnic@math.usc.edu.

[1] Partially supported by NSF.

SSDI 0022-4049(94)00128-6

In this paper we show that this is indeed the case when $r = 2$ (Theorems 5.1 and 5.2, Corollary 5.3). Here are some of the results.

If E_1, E_2 are subfields of K with $k \subset E_i \subset K$, then for any positive integer n, the n-torsion subgroup of $K^*/E_1^*E_2^*$ is finite, and it has no p-torsion for $p = \mathrm{char}(k)$.

If l is an odd prime, and k contains the lth roots of unity, then the l-primary torsion subgroup of $K^*/E_1^*E_2^*$ is finite. The analogous result holds true for the 2-primary subgroup if the 4th roots of unity are in k.

Let $\mu(K)$ denote the roots of unity in K. The torsion group of $K^*/E_1^*E_2^*$ is infinite if and only if $\mu(K)/\mu(E_1)\mu(E_2)$ is infinite (Theorem 5.2). In particular, if k (or E_i) contains all roots of unity, then the torsion subgroup of $K^*/E_1^*E_2^*$ is finite.

If k is finitely generated over its prime subfield, then the whole torsion subgroup of $K^*/E_1^*E_2^*$ is finite.

For $r \geq 3$, such finiteness statements no longer hold (see Example 6.4 or [7, 1.2] for an example with $r = 3$ where the quotient group is an infinite group of exponent 2). For arbitrary $r \geq 1$, for ℓ an odd prime number, when the ℓth roots of unity are in k, we show that the ℓ-primary torsion subgroup of $K^*/E_1^* \cdots E_r^*$ is of bounded exponent (Corollary 6.2) and that this subgroup is finite if $r = 2$ (Corollary 5.3).

Similar (but weaker) finiteness results in the case $r = 2$ were first arrived at by recourse to Picard groups of singular curves [9, 20].

The point of the present paper is to get at these finiteness results (and obtain the stronger ones mentioned above – in particular, results relating to the finiteness of the torsion subgroup and to the triviality of the p-torsion subgroup) in a direct fashion – essentially by means of Galois cohomology and such standard tools as Hilbert's theorem 90 (of course, the results on fields finitely generated over the prime field also make use of deep classical results). Given k, K, E_i $(i = 1, \ldots, r)$ as above, L/k the Galois closure of K/k, and $G = \mathrm{Gal}(L/k)$, there are naturally associated G–modules of finite type S and T (see Section 2), and the quotient $K^*/E_1^* \cdots E_r^*$ is related to the Galois cohomology of some associated G-modules. For $r = 2$, the finiteness theorems follow from purely algebraic facts: the module T is torsion-free and S is a permutation lattice (Theorem 2.6; see also Theorem 3.6).

The abelian groups $K^*/E_1^* \cdots E_r^*$ have also been studied in other papers [2, 5, 7, 8, 17, 19]. In those papers, the emphasis is on the torsion-free rank of the abelian group $K^*/E_1^* \cdots E_r^*$ (the starting point being Brandis' result that if k is infinite, then the quotient K^*/k^* is not finitely generated). If $r \leq 2$, then this quotient has infinite torsionfree rank (see [19, 1.2], [7, 5.5] or Theorem 5.10). If $r \geq 3$, then there are examples with this quotient trivial, infinite torsion or of infinite torsionfree rank (see [7] and Sections 4, 6 and 7 below for various examples).

We first study the problem in the more general setting of a finite group acting on a module. Let G be a finite group and M a $\mathbf{Z}G$-module. Let $\mathscr{C}$ be a family of subgroups $C_1, \ldots, C_r$ of G with D a subgroup of the intersection. Let M^H denote the fixed points of H on M. Let $\lambda(M) = \lambda_{\mathscr{C}}(M) = \Sigma_{i=1}^r M^{C_i} \subseteq M^D$. We study the abelian group structure of $M^D/\lambda(M)$ and in particular its torsion subgroup. If $r = 2$ and $H = \langle C_1, C_2 \rangle$, we show that the structure of the torsion subgroup depends upon $H^1(H, M)$ and the torsion

subgroup of M. If both these groups are finite, then the torsion subgroup of $M^D/\lambda(M)$ is finite (Corollary 2.8).

In Section 5 (for the case of two subfields) and Section 6 (for the general case), we use the group theoretic results (applied to Galois groups) together with cohomological information about fields to obtain the main results on fields mentioned above. In Section 7, we outline another approach to the case of fields finitely generated over the prime field.

In a sequel [6], we will explore the relationship between some of the results established here and Picard groups.

2. Fixed points on modules

Fix a finite group G. Unless noted otherwise, all G-modules will be left G-modules and all tensor products will be over $\mathbf{Z}$. Recall that if M and N are G-modules, then so are $M\otimes N$ (with $g(m\otimes n) = gm\otimes gn$) and $\mathrm{Hom}_{\mathbf{Z}}(M,N)$ (with $(gf)(m) = g(f(g^{-1}m))$. If A is a subgroup of G, let X_A denote the $\mathbf{Z}G$ permutation lattice on the left cosets of A (note that X_A is just the induced module $\mathbf{Z}[G/A] = \mathbf{Z}G\otimes_{\mathbf{Z}A}\mathbf{Z}$. If $g\in G$, let $\bar{g}$ denote the left coset gA. If M is a G-module, let M^G denote the fixed points of G on M. Note that if M is any G-module, then M^A and $(M\otimes X_A)^G$ can be naturally identified as abelian groups via $x\to \Sigma gx\otimes\bar{g}$, where the sum is over a set of coset representatives for the left cosets of A.

If $A\subseteq B$ are subgroups of G, then there is a homomorphism $\varphi = \varphi_{A,B}$ of G-sets from G/A onto G/B (given by $\varphi(gA) = gB$). This induces a homomorphism (which we also denote by φ) from X_A onto X_B. Let $\gamma = \gamma_{A,B} : X_B \to X_A$ be the map on the duals induced by φ (note any permutation lattice is self dual). Explicitly, $\gamma(gB) = \Sigma_{i=1}^{s} gb_iA$, where $b_1,\ldots,b_s$ are left coset representatives for B/A. For example, if $A = 1$ and $B = H$, then the map $\mathbf{Z}[G/H]\to\mathbf{Z}[G]$ is the G-map which sends $\bar{1}$ to $N_H := \Sigma_{h\in H}h$. Note that γ is a split injection of abelian groups.

If M is any $\mathbf{Z}G$-module, then there is an induced injection $1\otimes\gamma : M\otimes X_B\to M\otimes X_A$. This induces a mapping on G-fixed points and via the identification above induces the inclusion $M^B\to M^A$.

The maps γ and φ induce the short exact sequences

$$0\to X_B\xrightarrow{\gamma} X_A\to V\to 0, \tag{1}$$

$$0\to V'\to X_A\xrightarrow{\varphi} X_B\to 0. \tag{1'}$$

We note that V' is a free abelian group of rank $[G:A]-[G:B]$. Since (1) and (1′) are dual to one another, the same is true for V.

Since (1) is split exact as a sequence of abelian groups, we can tensor with any $\mathbf{Z}G$-module M and obtain:

$$0\to M\otimes X_B\to M\otimes X_A\to M\otimes V\to 0. \tag{2}$$

Taking G-fixed points, and using the identification above and the isomorphism $H^1(G, M \otimes X_B) \cong H^1(B, M)$ (Shapiro's Lemma, cf. [3, Proposition 6.2, p. 73]), we get:

$$0 \to M^B \to M^A \to (M \otimes V)^G \to H^1(B, M). \tag{3}$$

If we take $(A, B) = (C, G)$ above, this yields:

Lemma 2.1. *Let C be a subgroup of the finite group G. Let M be a G-module. Then M^C/M^G embeds into M^s, where $s = [G : C] - 1$.*

Next we consider the situation of a family of subgroups. Let $\mathscr{C} = \{C_i : 1 \leq i \leq r\}$ be a family of subgroups of the finite group G. Let $D \subseteq \bigcap_{i=1}^r C_i$ be a subgroup of G. Let $X_i = X_{C_i}$ and $\gamma_i = \gamma_{D,C_i}$. Let $\gamma : X_1 \oplus \cdots \oplus X_r \to X_D$ be defined by $\gamma(x_1, \ldots, x_r) = \gamma_1(x_1) + \ldots + \gamma_r(x_r)$. Set $X = X_1 \oplus \cdots \oplus X_r$.

This yields the basic exact sequence of G-modules

$$0 \to S \to X \xrightarrow{\gamma} X_D \to T \to 0. \tag{4}$$

Here $S = \ker(\gamma)$ and $T = \operatorname{coker}(\gamma)$. Note that when $r = 1$, (4) is essentially (1). In particular, for $r = 1$, $S = 0$ and T is torsionfree.

Let $Y = \gamma(X)$. It is convenient to break up sequence (4) into two short exact sequences:

$$0 \to S \to X \xrightarrow{\gamma} Y \to 0, \tag{5}$$

$$0 \to Y \to X_D \to T \to 0. \tag{6}$$

Since $Y \subseteq X_D$, the abelian group Y is free and so (5) is always split exact in the category of abelian groups.

Let M be a $\mathbf{Z}G$-module. Let $\lambda(M) = \Sigma_{i=1}^r M^{C_i} \subseteq M^D$. We are interested in the structure of the abelian group $M^D/\lambda(M)$. Let $\alpha = 1 \otimes \gamma : M \otimes X \to M \otimes X_D$. Let $N \subseteq M \otimes X_D$ be the image of $M \otimes X$ under α. Since we are identifying $(M \otimes X_i)^G$ with M^{C_i}, we see that $\alpha((M \otimes X)^G) = \lambda(M) \subseteq N^G \subseteq (M \otimes X_D)^G = M^D$. Thus

$$M^D/\lambda(M) \cong \operatorname{coker}(\alpha : (M \otimes X)^G \to M^D).$$

Tensoring M with (5) yields a short exact sequence:

$$0 \to M \otimes S \to M \otimes X \xrightarrow{\alpha} M \otimes Y \to 0. \tag{7}$$

Taking fixed points yields:

$$0 \to (M \otimes S)^G \to (M \otimes X)^G \xrightarrow{\alpha} (M \otimes Y)^G \to H^1(G, M \otimes S) \to H^1(G, M \otimes X). \tag{8}$$

From now on, assume that one of the two abelian groups M and T is torsionfree, hence flat. If T is torsionfree, then (6) is split exact as a sequence of abelian groups

and in fact $N = M \otimes Y$ – similarly, if M is torsionfree, then $M \otimes Y$ injects into $M \otimes X_D$ and so $N = M \otimes Y$. Thus (8) yields:

$$0 \to N^G/\lambda(M) \to H^1(G, M \otimes S) \to \bigoplus_{i=1}^{r} H^1(C_i, M). \tag{8'}$$

Tensoring M with (6) yields the short exact sequence:

$$0 \to N \to M \otimes X_D \to M \otimes T \to 0. \tag{9}$$

Taking G-fixed points yields:

$$0 \to N^G \to M^D \to (M \otimes T)^G \to H^1(G, N) \to H^1(D, M), \tag{10}$$

and

$$0 \to M^D/N^G \to (M \otimes T)^G \to H^1(G, M \otimes Y) \to H^1(D, M). \tag{10'}$$

Set $M_1 = N^G$. By (10'), M^D/M_1 embeds into $(M \otimes T)^G$. By (8'), $M_1/\lambda(M)$ embeds into $H^1(G, M \otimes S)$ (and in particular is a torsion group of exponent dividing $|G|$). Thus:

Theorem 2.2. *Let G be a finite group with subgroups $C_i, 1 \leq i \leq r$. Let D be a subgroup of $\cap_i C_i$. Let the G-modules S and T be defined as in* (4). *Let M be a $\mathbf{Z}G$-module and assume that either M or T is $\mathbf{Z}$-torsionfree. Let $\lambda(M) = \Sigma_{i=1}^{r} M^{C_i} \subseteq M^D$. Then there exists a subgroup M_1 of M^D containing $\lambda(M)$ such that*

(a) *M^D/M_1 embeds into $(M \otimes T)^G \subseteq (M \otimes T)$, and*

(b) *$M_1/\lambda(M)$ embeds into $H^1(G, M \otimes S)$.*

A G-module M is called coflasque if $H^1(C, M) = 0$ for all subgroups C of the finite group G. Permutation lattices are coflasque (by Shapiro's Lemma). If M is any abelian group, let $\mu(M) = M_{\text{tors}}$ be its torsion subgroup.

Corollary 2.3. *Keep notation and assumptions as in the previous theorem.*

(a) *If T is torsionfree and the torsion subgroup of M has exponent d, then the torsion subgroup of $M^D/\lambda(M)$ has exponent dividing de, where $H^1(G, M \otimes S)$ has exponent e. Note that e always divides $|G|$.*

(b) *If T or M is torsionfree and $H^1(G, M \otimes S) = 0$, then $M^D/\lambda(M)$ embeds into $(M \otimes T)^G \subseteq (M \otimes T)$. If in addition, T is torsionfree, then $\mu(M^D/\lambda(M))$ embeds into $(\mu(M) \otimes T)^G$.*

(c) *If M and T are both torsionfree, then the torsion subgroup of $M^D/\lambda(M)$ embeds into $H^1(G, M \otimes S)$.*

(d) *If M is torsionfree, then the torsion subgroup of $M^D/\lambda(M)$ has exponent dividing te, where t is the exponent of the torsion subgroup of T and e is the exponent of $H^1(G, M \otimes S)$.*

(e) *If M is torsionfree and coflasque and T is torsionfree, then the torsion subgroup of $M^D/\lambda(M)$ is isomorphic to $H^1(G, M \otimes S)$. In particular, if $M = X_C$ for some*

subgroup C of G and T is torsionfree, then the torsion subgroup of $M^D/\lambda(M)$ is isomorphic to $H^1(C,S)$.

(f) *If $M = \mathbf{Z}G$, then $M^D/\lambda(M) \cong T$.*

(g) *If $T = 0$ and $D = 1$, then $M/\lambda(M)$ embeds into $H^1(G, M \otimes S)$. If, in addition, M is coflasque, then $M = \lambda(M)$.*

Proof. (a)–(d) are immediate consequences of the previous theorem. Assume that both M and T are torsionfree and that M is coflasque. By (10′), M^D/N^G is torsionfree and so the torsion subgroup is isomorphic to $N^G/\lambda(M)$. Since M is coflasque, $H^1(G, M \otimes X) = 0$ and so (8′) yields $N^G/\lambda(M) \cong H^1(G, M \otimes S)$. This proves the first assertion of (e). The last statement of (e) now follows by Shapiro's Lemma.

Now consider the case $M = \mathbf{Z}G$. Since $H^1(G, M \otimes S) = 0$, (8′) implies that $N^G = \lambda(M)$. Since $H^1(G, M \otimes Y) = 0$, it follows from (10′) that $M^D/\lambda(M) \cong (M \otimes T)^G \cong T$.

If $T = 0$ and $D = 1$, then $M = M^D = M_1$. Thus, the first statement follows from the previous theorem. Moreover, (4) splits when $T = 0$ and $D = 1$. It follows that S is a summand of X_D, and so if M is coflasque, then $H^1(G, M \otimes S) = 0$. Thus (g) follows. □

In general, given a family of subgroups as above, T is not torsionfree. Moreover, there is little reason to expect that $H^1(G, M \otimes S)$ should be 0. We note, however, that S satisfies:

Theorem 2.4. *Let S be defined as in* (4). *Then $H^1(G,S) = 0$.*

Proof. By taking fixed points on (5) and using $H^1(G,X) = 0$, we see that it suffices to show that $\gamma(X^G) = Y^G$. This in turn follows from the fact that γ_i induces a surjection of the rank-one submodule $(X_{C_i})^G$ to $(X_D)^G$. □

We will show below (Example 2.9) that S need not always be coflasque (even if T is torsionfree). See Corollary 2.3(e) above and Theorem 7.2 for the relevance of this condition. When $r = 1$, $S = 0$. In the case of two subgroups, the groups S and T are still quite controlled, as we shall now see.

So keep notation as above and assume $r = 2$. Set $H = \langle C_1, C_2 \rangle$. We will prove that in this case T is torsionfree and that $S \cong X_H$ (and in particular is coflasque). See Section 3 for a different proof. We first prove that T is torsionfree.

Proposition 2.5. *Let Γ be a finite G-set. Set $H = \langle C_1, C_2 \rangle$. Set $s = t + u - v_1 - v_2$, where $t = |\Gamma|$, C_i has v_i orbits on Γ and H has u orbits on Γ.*

(a) *Let M be the $\mathbf{Z}G$-permutation lattice on Γ. Then $M/(M^{C_1} + M^{C_2})$ is free of rank s.*

(b) *Let U be an abelian group. Let W be the abelian group of functions from Γ to U viewed as a G-module via its action on Γ. (So $W = U \times \cdots \times U$ and G acts via permuting the coordinates.) Then $W/(W^{C_1} + W^{C_2}) \cong U^s$.*

Proof. (a) We note that a subgroup N of a finitely generated free abelian group M is a direct summand if and only if $d(p)$, the dimension of $(N/N \cap pM)$ over the prime field, is independent of the prime p. We apply this criterion to $N = M^{C_1} + M^{C_2}$.

Fix a prime p and set $\bar{M} = M/pM$. If L is a subgroup of M, let $\bar{L}$ denote its image in $\bar{M}$. Let π be the natural projection of M onto $\bar{M}$.

We identify Γ with a permutation basis for M (i.e. it is a basis and is G-invariant). If C is a subgroup of G, then observe that a basis for M^C consists of $\Sigma\omega$, where the sum is over ω in a C-orbit of Γ. Observe that this is true for a permutation lattice over any commutative ring.

This implies that $\pi(M)^C = \pi(M^C)$ and has dimension equal to $f(C)$, where $f(C)$ is the number of orbits of C on Γ (and in particular is independent of p).

Clearly $\bar{M}^{C_1} \cap \bar{M}^{C_2} = \bar{M}^H$ has dimension u. Thus $\pi(N) = \bar{M}^{C_1} + \bar{M}^{C_2}$ has dimension $v_1 + v_2 - u$ and in particular is independent of p. Hence N is a summand of M of rank $v_1 + v_2 - u$ and M/N is free of rank $t + u - v_1 - v_2$.

(b) Let M be the permutation lattice on Γ. Thus $W = M \otimes U$ where G acts trivially on U. If C is a subgroup of G, then $W^C = M^C \otimes U$. Thus, since $M^{C_1} + M^{C_2}$ is an abelian group summand of M, $W^{C_1} + W^{C_2} = (M^{C_1} + M^{C_2}) \otimes U$. Hence $W/(W^{C_1} + W^{C_2}) = [M/(M^{C_1} + M^{C_2})] \otimes U \cong U^s$ by (a). □

The next result, for $r = 2$, identifies S and shows T is torsionfree.

Theorem 2.6. *Let G be a finite group with subgroups D, C_1 and C_2 with $D \subseteq C_1 \cap C_2$. Let $H = \langle C_1, C_2 \rangle \subseteq G$. In the exact sequence*

$$0 \to S \to X_{C_1} \oplus X_{C_2} \xrightarrow{\gamma_1 + \gamma_2} X_D \to T \to 0$$

given by (4) *for $r = 2$, $S \cong X_H = \mathbf{Z}[G/H]$ and T is torsionfree of rank $s = s(C_1, C_2, D) := [G : D] + [G : H] - [G : C_1] - [G : C_2]$.*

Proof. First note that the formula for the rank of T follows immediately from (4) once we have proved $S \cong X_H$ and so has rank $[G : H]$.

Let S_G and T_G denote the corresponding terms in (4) when $D = 1$. Since X_D embeds into X_E for any $E \subseteq D$ via $\gamma_{E,D}$ and since $\gamma_{E,D} \circ \gamma_{D,C_i} = \gamma_{E,C_i}$, it follows that $S = S_G$. Similarly, we see that T_D embeds into T_G. So we may and shall assume that $D = 1$ and so $X_D = \mathbf{Z}G$.

The fact that T is torsionfree follows from Proposition 2.5(a) and Corollary 2.3(f) applied to $M = \mathbf{Z}G$.

The image of γ_i is $\{\Sigma_{g \in G} a_g g : a_g = a_h \text{ if } gC_i = hC_i\}$. These are precisely the fixed points of C_i under the right regular representation of G on $\mathbf{Z}G$. Since γ_i embeds X_{C_i} into $X = X_G$, $S = \{(x_1, x_2) : \gamma_1(x_1) + \gamma_2(x_2) = 0\}$ can be identified with $\gamma_1(X_{C_1}) \cap \gamma_2(X_{C_2})$. As we observed above, this intersection is precisely the set of fixed points of H under the right representation of H on $\mathbf{Z}G$. This is clearly isomorphic (under the left action) to the permutation lattice X_H as desired. □

Thus Theorem 2.2 always applies when $r = 2$. By Shapiro's Lemma, we have $H^1(G, M \otimes X_H) \cong H^1(H, M)$. Theorem 2.2 gives:

Theorem 2.7. *Let D, C_1, C_2 be subgroups of the finite group G with $D \subseteq C_1 \cap C_2$. Set $H = \langle C_1, C_2 \rangle$. There exists a short exact sequence of abelian groups*

$$0 \to U \to M^D/(M^{C_1} + M^{C_2}) \to V \to 0,$$

where U is a subgroup of $H^1(H, M)$ and V is a subgroup of M^s, where s is the integer defined in Theorem 2.6.

Corollary 2.8. *Let D, C_1, C_2 be subgroups of the finite group G with $D \subseteq C_1 \cap C_2$. Set $H = \langle C_1, C_2 \rangle$.*

(a) *If $H^1(H, M) = 0$, then $M^D/(M^{C_1} + M^{C_2})$ embeds into M^s. If, moreover, M is torsionfree, then so is $M^D/(M^{C_1} + M^{C_2})$.*

(b) *If $H^1(H, M)$ is finite and the torsion subgroup of M is finite, then the torsion subgroup of $M^D/(M^{C_1} + M^{C_2})$ is finite.*

We will consider applications to fields in later sections. Let us just point out that Corollary 2.8(a) applies when M is the multiplicative group of a field and G is a finite group of field automorphisms.

We now give an example where S is not coflasque but T is torsionfree.

Example 2.9. Let G be an elementary abelian group of order 8 with generators $x_i, 1 \leq i \leq 3$. Set $C_i = \langle x_i \rangle$ and $D = 1$. Let $C = \langle y \rangle$, where $y = x_1x_2x_3$. Let S and T be defined by (4).

(a) T is an infinite cyclic group and g acts via multiplication by $\rho(g)$, where ρ is the character on G with $\rho(x_i) = -1$ for all i.

(b) $|H^1(C, S)| = 2$.

Proof. Keep notation as in (4). Let Y be the image of γ. Consider the basis $1, x_1, x_2, x_1x_2, x_3, x_1x_3, x_2x_3, y$ for $\mathbf{Z}G$, and the bases for X_i in compatible order. Then the matrix of γ with respect to these bases is

$$\begin{pmatrix} 1&0&0&0&1&0&0&0&1&0&0&0 \\ 1&0&0&0&0&1&0&0&0&1&0&0 \\ 0&1&0&0&1&0&0&0&0&0&1&0 \\ 0&1&0&0&0&1&0&0&0&0&0&1 \\ 0&0&1&0&0&0&1&0&1&0&0&0 \\ 0&0&1&0&0&0&0&1&0&1&0&0 \\ 0&0&0&1&0&0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1 \end{pmatrix}.$$

It is straightforward to compute that the rank of this matrix is 7 modulo p for every prime p (if p is odd, then Y/pY is complemented by the one-dimensional irreducible

representation with character ρ – if $p = 2$, then one computes directly that the matrix has rank 7). It follows that Y is an abelian group summand of $\mathbf{Z}G$ of rank 7. Thus T is infinite cyclic. Since the irreducible representation of G with character ρ is not a constituent of X, it must occur on T. Thus (a) holds.

Since $T^C = 0$, it follows that $Y^C = (\mathbf{Z}G)^C$. A straightforward computation shows that $|Y^C/\gamma(X^C)| = 2$ (indeed, to see that $\gamma(X^C) \neq Y^C$, just observe that $\varepsilon(\gamma(w)) \equiv 0 \pmod 4$ for every $w \in X^C$, but $\varepsilon(1 + y) = 2$, where $\varepsilon : \mathbf{Z}G \to \mathbf{Z}$ is the augmentation map – thus, $1 + y \in Y^C - \gamma(X^C)$). Consider the sequence (5). Taking C-fixed points yields:

$$0 \to S^C \to X^C \xrightarrow{\gamma} Y^C \to H^1(C,S) \to H^1(C,X) = 0.$$

Thus, $H^1(C,S) \cong Y^C/\gamma(X^C)$ and (b) follows. □

The next result shows that in some cases with $r \geq 3$, S may be coflasque. A $\mathbf{Z}G$-lattice is called invertible if it is a summand of a permutation lattice. Since permutation lattices are coflasque, so are invertible lattices.

Proposition 2.10. *Let $C_1, \ldots, C_r$ be subgroups of G. Let S and T be defined by* (4).

(a) *Assume that $G = C_iC_j$ for each $i \neq j$. Then S is a trivial $\mathbf{Z}G$-lattice of rank $r - 1$.*

(b) *If $D = 1$ and $T = 0$, then S is invertible.*

Proof. (a) It suffices to prove that G acts trivially on $S \otimes \mathbf{Q}$ and that this vector space has dimension $r - 1$. The hypothesis implies that $\mathbf{Q}[G/C_i]$ and $\mathbf{Q}[G/C_j]$ have only the trivial irreducible constituent in common. Since each γ_i is injective, this implies that $S \otimes Q$ contains no nontrivial constituents. It remains only to compute the dimension. Since $\mathbf{Q}[G/D]$ has only a one-dimensional fixed space which is in the image of γ, the result follows.

Sequence (4) splits for $T = 0$ and $D = 1$. Thus (b) follows. □

Part (a) of the previous result applies when the C_i are any collection of maximal subgroups of a nilpotent group G or more generally any collection of pairwise non-conjugate maximal subgroups of a solvable group G (see [1, Corollary 1]).

If the C_i are the collection of all nontrivial subgroups of G, then T is quite often zero. In particular, this is true for G any nonabelian simple group. See [7, Section 4].

Lemma 2.11. *Let M be a $\mathbf{Z}G$-module. Let $f : M \to M \otimes \mathbf{Z}G$ be the injective G-module map defined by $f(m) = \Sigma_{g \in G} m \otimes g$. Let F be any additive functor from G-modules to abelian groups. Then f induces the natural map π from $F(M)$ to $F(M \otimes \mathbf{Z}G)$ and* $\ker(\pi)$ *has exponent dividing $|G|$.*

Proof. Let $|G| = n$. The composite G-map

$$\mathbf{Z} \to \mathbf{Z}[G] \to \mathbf{Z}$$

(the first map is the norm, the second the augmentation map) is multiplication by n. Now tensor this sequence by any G-module M. The composite map is still multiplication by n. Since F is additive, the composite map $F(M) \to F(M \otimes \mathbf{Z}G) \to F(M)$ is multiplication by n, and the kernel of the map $F(M) \to F(M \otimes \mathbf{Z}G)$ is killed by n. □

Later (see Proposition 6.3) we will apply the previous result to the functor F defined by $F(M) = M^D/\lambda(M)$.

We now investigate to what extent the torsion subgroup of $M/\lambda(M)$ is determined by the torsion subgroup of M. We first prove an easy cohomological result. Recall that a group is locally $\mathscr{P}$ for some property $\mathscr{P}$ if every finitely generated subgroup has property $\mathscr{P}$. We use the notation D^iG for the ith derived group of D.

Lemma 2.12. *Let G be a finite group. Let M be a $\mathbf{Z}G$-module which is locally d-generated as an abelian group. Let K be a normal subgroup of G acting trivially on M.*

(a) *$H^1(G,M)$ is finite and has order dividing $|G/D^1K|^d$.*

(b) *If $d = 1$, then $H^1(G,M)$ has finite order dividing $|G/D^2G|$.*

Proof. Recall that if H is a normal subgroup of G, then one has the restriction–inflation exact sequence (cf. [18, Proposition 4, p.117])

$$0 \to H^1(G/H, M^H) \to H^1(G,M) \to H^1(H,M)^G.$$

Set $R = H^1(G,M)$. We first prove the apparently weaker result that $|R|$ divides $|G|^d$. We prove this by induction on $|G|$. First assume that $G = \langle g \rangle$ is cyclic of order m. Then it is straightforward to show that R is isomorphic to a subgroup of $M/(g-1)M$ (a derivation δ of G into M is determined by $\delta(g)$; δ is inner if and only if $\delta(g) \in (g-1)M$). Since R has exponent dividing m, it embeds into the m-torsion subgroup of $M/(g-1)M$. Since M is locally d-generated, the same is true of $M/(g-1)M$. In particular, the m-torsion subgroup has order dividing m^d and the result holds in this case.

The result now holds for any solvable group by induction and the restriction–inflation sequence above.

Since R is a torsion group, it suffices to consider the p-primary subgroup $R(p)$ of R for each prime p. Then res : $R(p) \to H^1(P,M)$ is injective for a Sylow p-subgroup P of G (cf. [3, 10.3, p. 84]). Thus, we have proved $|H^1(G,M)|$ divides $|G|^d$.

We now prove (a). Apply the restriction–inflation sequence with $H = K$. Then it follows that $|R|$ divides

$$|H^1(G/K,M)||H^1(K,M)^G|.$$

Since K acts trivially on M, $H^1(K,M)^G \cong \mathrm{Hom}(K/DK,M)^G$. Now (a) follows from the facts that $|\mathrm{Hom}(K/DK,M)|$ divides $|K/DK|^d$ (this reduces to the case K is cyclic) and that $|H^1(G/K,M)|$ divides $|G/K|^d$.

Finally assume $d = 1$. Thus D^1G acts trivially on M (the automorphism group of a locally cyclic group is abelian). Thus (a) with $K = D^1G$ implies (b). □

Let G be a finite group with subgroups $C_1, \ldots, C_r$ and $D \subseteq \bigcap_i C_i$. Let S and T be defined as in (4). Let M be a G-module and let $\mu(M)$ denote its torsion subgroup. Set $L = M/\mu(M)$ and $\pi : M \to L$. Let $M_i = M^{C_i}$ and $L_i = L^{C_i}$. We conclude from the exact sequence

$$0 \to \mu(M_i) \to M_i \to L_i \to H^1(C_i, \mu(M))$$

that there exists a surjection $V = \bigoplus_i V_i \to (\lambda(L)/\pi(\lambda(M))$ where V_i is a subgroup of $H^1(C_i, \mu(M))$. In particular, $(\lambda(L)/\pi(\lambda(M))$ is a torsion group and so is a subgroup of $J := (L^D/\pi(\lambda(M))_{\text{tors}}$.

Set R equal to the cokernel of the natural map

$$f : \mu(M^D)/\lambda(\mu(M)) \to (M^D/\lambda(M))_{\text{tors}}.$$

So $R \cong (M^D/(\lambda(M) + \mu(M^D)))_{\text{tors}}$ is isomorphic (via the map induced by π) to a subgroup of J.

Now consider the short exact sequence

$$0 \to \lambda(L)/\pi(\lambda(M)) \to J \to (L^D/\lambda(L))_{\text{tors}} \to 0. \qquad (*)$$

The left-hand group is a homomorphic image of V (and so has exponent dividing $|G|$), and the right-hand group has exponent dividing $t|G|$ where t is the exponent of the torsion subgroup of T (Corollary 2.3(d)). Thus J (and so R) has exponent dividing $t|G|^2$. So we have shown:

Proposition 2.13. *Let G be a finite group with subgroups C_i, $i = 1, \ldots, r$, and $D \subset \bigcap_i C_i$. Let M be a $\mathbf{Z}G$-module with torsion subgroup $\mu(M)$. The natural map*

$$f : \mu(M^D)/\lambda(\mu(M)) \to (M^D/\lambda(M))_{\text{tors}}$$

has cokernel of finite exponent dividing $t|G|^2$ where t is the exponent of the torsion subgroup of T (as in (4)).

If T is torsionfree (e.g., if $r \leq 2$), then we can obtain more precise formulations of the previous result. In $(*)$ above, it follows by Corollary 2.3(c) that the right-hand group is a subgroup of $H^1(G, L \otimes S)$. This yields:

Theorem 2.14. *Let G be a finite group with subgroups C_i, $i = 1, \ldots, r$, and $D \subset \bigcap_i C_i$. Let $H = \langle C_1, \ldots, C_r \rangle$. Let M be a $\mathbf{Z}G$-module with torsion subgroup $\mu(M)$. Let S and T be defined by (4). Assume that T is torsionfree (e.g., $r \leq 2$).*

(a) *The natural map*

$$f : \mu(M^D)/\lambda(\mu(M)) \to (M^D/\lambda(M))_{\text{tors}}$$

has cokernel R of exponent dividing $|G|^2$, and there exists a short exact sequence

$$V \to R \to U \to 0,$$

where V is a subgroup of $\bigoplus_i H^1(C_i, \mu(M))$ and U is a subgroup of $H^1(G, (M/\mu(M)) \otimes S)$.

(b) *If all the cohomology groups in* (a) *are finite, then $|R|$ divides*

$$|H^1(G, (M/\mu(M)) \otimes S)||H^1(C_1, \mu(M))| \cdots |H^1(C_r, \mu(M))|.$$

(c) *If $r = 2$ and the cohomology groups in* (a) *are finite, then $|R|$ divides*

$$|H^1(C_1, \mu(M))||H^1(C_2, \mu(M))||H^1(H, M/\mu(M)|.$$

(d) *If $r = 1$, then R is a homomorphic image of $H^1(C_1, \mu(M))$. In particular, if $\mu(M)$ is locally d-generated, R has order dividing $|C_1|^d$.*

(e) *If $r = 1$, $D = 1$ and $C_1 = G$, then $R \cong \ker(H^1(G, \mu(M)) \to H^1(G, M))$.*

Proof. (a) and (b) are immediate consequences of (*) and our previous observations. If $r = 2$, then T is torsionfree and $S = X_H$, whence (c) follows from (b). If $r = 1$, then (4) is essentially (1), and $S = 0$ and T is torsionfree. Thus (d) follows from (a), (b) and Lemma 2.12.

(e) Under the hypotheses of (e), $R = J$ and $L/\lambda(L)$ is torsionfree. Thus, by (*), $R \cong L^G/\pi(M^G)$ and the result follows from the long cohomology sequence. □

We close this section with a simple remark about the torsionfree rank of $M^D/\lambda(M)$. Since for this purpose we may replace M by $\mathbf{Q} \otimes M$, we may assume that M is a $\mathbf{Q}G$-module. An immediate consequence of (8) and (10) is the following result.

Proposition 2.15. *Let M be a $\mathbf{Q}G$-module.*

(a) $M^D/\lambda(M) \cong (M \otimes T)^G$.

(b) *If T is infinite (e.g., if $r \leq 2$) and M contains every irreducible $\mathbf{Q}G$-module, then $M^D/\lambda(M)$ is nonzero.*

(c) *If T is infinite and M contains every irreducible $\mathbf{Q}G$-module as a summand with infinite multiplicity, then $M^D/\lambda(M)$ has infinite dimension over $\mathbf{Q}$.*

Proof. We first apply (10). Since M and N are $\mathbf{Q}G$-modules, (10) reduces to a short exact sequence. Thus $M^D/N^G \cong (M \otimes T)^G$. Since $H^1(G, M \otimes S) = 0$, it follows from (8) that $N^G = \lambda(M)$. Thus (a) holds.

Assume that T is infinite. Let V be an irreducible $\mathbf{Q}G$-summand of $\mathbf{Q} \otimes T$. By assumption, the dual V^* of V is a $\mathbf{Q}G$-summand of M. Thus $(V^* \otimes V)^G$ is a nonzero submodule of $(M \otimes T)^G$. Now (b) follows from (a).

If $r \leq 2$, then T is infinite (see Theorem 2.6 – the part of the proof showing that T has positive rank is quite easy).

The proof of (c) is analogous to that of (b). □

3. A dual approach

There is a dual version of some of the results of the previous section. Instead of considering $\gamma : X \to X_D$ in (4), we consider the dual map $\varphi : X_D \to X$ given explicitly by $\varphi = (\varphi_1, \ldots, \varphi_r)$, where $\varphi_i = \varphi_{D,C_i}$. This yields the exact sequence:

$$0 \to T' \to X_D \to X \to S' \to 0. \tag{11}$$

Note that (11) is almost dual to (4). Indeed, they will be dual if S' or T is torsionfree via the "duality" $M \to \mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Z})$. If T is torsionfree, then (4) is split exact as a sequence of abelian groups. Therefore, applying this duality yields (11), which is also split exact as a sequence of abelian groups. Thus S' is torsionfree. Similarly, if S' is torsionfree, T is also torsionfree. So S' is torsionfree if and only if T is torsionfree. In any case, the sequences become dual to one another after we tensor with $\mathbf{Q}$.

We can recover some of the previous results by applying the functor $\mathrm{Hom}_G(\,.\,, M)$. Note that $\mathrm{Hom}_G(X_i, M)$ can be identified with M^{C_i}. Similarly, $\mathrm{Hom}_G(X_D, M) = M^D$. Thus, the map $X_D \to X$ induces a map from $\mathrm{Hom}_G(X, M) \to \mathrm{Hom}_G(X_D, M)$ and the cokernel of this map is $M^D/\lambda(M)$.

Let $Y' = \varphi(X_D)$. It is convenient to break up (11) into short exact sequences:

$$0 \to Y' \to X \to S' \to 0, \tag{12}$$

and

$$0 \to T' \to X_D \to Y' \to 0. \tag{13}$$

Let M be a $\mathbf{Z}G$-module. We apply the functor $\mathrm{Hom}_G(\,.\,, M)$ to (12) and (13). This yields:

$$\begin{aligned} 0 \to \mathrm{Hom}_G(S', M) \to \mathrm{Hom}_G(X, M) \to \mathrm{Hom}_G(Y', M) \\ \to \mathrm{Ext}^1_G(S', M) \to \mathrm{Ext}^1_G(X, M) \end{aligned} \tag{14}$$

and

$$\begin{aligned} 0 \to \mathrm{Hom}_G(Y', M) \to \mathrm{Hom}_G(X_D, M) \to \mathrm{Hom}_G(T', M) \\ \to \mathrm{Ext}^1_G(Y', M) \to \mathrm{Ext}^1_G(X_D, M). \end{aligned} \tag{15}$$

The identification mentioned above and (14) and (15) yield the analogue of Theorem 2.2. We can take $M_1 = \mathrm{Hom}_G(Y', M)$ in the next result.

Theorem 3.1. *Let G be a finite group with subgroups $C_i, 1 \le i \le r$. Let D be a subgroup of $\bigcap_i C_i$. Let S' and T' be defined as in* (11). *Let M be a $\mathbf{Z}G$-module. Then there exists a subgroup M_1 of M^D containing $\lambda(M)$ such that*

(a) *M^D/M_1 embeds into* $\mathrm{Hom}_G(T', M)$,

(b) *$M_1/\lambda(M)$ embeds into* $\mathrm{Ext}^1_G(S', M)$, *and*

(c) *the cokernel of the embedding in* (b) *is isomorphic to a subgroup of* $\mathrm{Ext}^1_G(X, M)$.

If T (or equivalently S') is torsionfree, then Theorems 3.1 and 2.2 give essentially identical information.

Corollary 3.2. *If M is torsionfree, then the torsion subgroup of $M/\lambda(M)$ is isomorphic to a subgroup of* $\mathrm{Ext}^1_G(S', M)$.

Proof. Let M_1 be as in Theorem 3.1. If M is torsionfree, then M/M^D and $\mathrm{Hom}_G(T', M)$ are both torsionfree. Thus, by 3.1(a) the torsion subgroup of $M/\lambda(M)$ is contained in $M_1/\lambda(M)$. The result follows from 3.1(b). □

One case which appears easier to deal with in this guise occurs when $T' = 0$ (or equivalently T is finite). We first record:

Lemma 3.3. *The following conditions are equivalent*:

(i) $T' = \ker \varphi = 0$ *in sequence* (11);

(ii) T *in sequence* (4) *is finite*;

(iii) $\mathrm{Im}(\gamma) \cap \mathbf{Z} \neq 0$, *where* $\mathbf{Z} \subset X_D = \mathbf{Z}[G/D]$ *via the obvious map* $1 \mapsto \bar{1}$.

Proof. The equivalence of (i) and (ii) follows from the fact that (4) and (11) become dual to one another after we tensor with $\mathbf{Q}$. If T is finite, then $\mathrm{Im}(\gamma)$ has finite index in X_D. Thus (ii) implies (iii). Assume (iii) holds. Choose a nonzero integer n with $n\bar{1}$ in the image of γ. Since $\bar{1}$ generates X_D as a G-module, this implies that the image of γ contains nX_D and so T is finite. □

Corollary 3.4. *Assume that $\gamma : X \to X_D$ has finite cokernel (or equivalently $\varphi : X_D \to X$ is injective).*

(a) $M^D/\lambda(M)$ *is isomorphic to a subgroup of* $\mathrm{Ext}^1_G(S', M)$. *In particular, it is a torsion group.*

(b) *If $H^1(C_i, M) = 0$ for each i, then $M^D/\lambda(M) \cong \mathrm{Ext}^1_G(S', M)$.*

Proof. (a) follows immediately from Theorem 3.1 (since $T' = 0$, $M^D = M_1$ in the notation of 3.1). Since X_i is a torsionfree abelian group, $\mathrm{Ext}^1_G(X_i, M) \cong H^1(G, \mathrm{Hom}_{\mathbf{Z}}(M, X_i))$ (cf. [3, p. 61]). Since $\mathrm{Hom}_{\mathbf{Z}}(M, X_i) \cong \mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Z}) \otimes X_i$ as G-modules, it follows by Shapiro's Lemma that $\mathrm{Ext}^1_G(X_i, M) \cong H^1(C_i, M) = 0$. Thus $\mathrm{Ext}^1_G(X, M) = 0$. It now follows from Theorem 3.1(c) that $M^D/\lambda(M) \cong \mathrm{Ext}^1_G(S', M)$. □

Assume for the moment that $D = 1$ and the family $\{C_i\}$ is the collection of all nontrivial subgroups of G (or all subgroups of prime order if G is not of prime order). This case has been studied in [7, 8]. Corollary 3.4(b) for this case is essentially contained in [8, Proposition 3.5].

Recall that a finite group G is called a Frobenius complement if there exists a nonzero $\mathbf{Q}G$-module V such that no nontrivial element of G fixes a nonzero element of V. In [7, Theorem 2.2] it was shown that T is torsion (or equivalently T' is zero) if and only if G is not a Frobenius complement. In the notation of [7, Section 1],

$\mathbf{I}(G)$ is the image of γ. Note that if the positive integer $s \in \mathbf{Z} \subset \mathbf{Z}[G]$ is in $\mathbf{I}(G)$, then $s = \Sigma a_C N_C$, where the sum is over all subgroups of prime order in G, $a_C \in \mathbf{Z}G$ and $N_C = \Sigma_{c \in C} c$. Applying this to any element m in the G-module M yields $sm \in \lambda(M)$ for all $m \in M$. Moreover [7, Theorem 3.1], when G is not a Frobenius complement, either $T = 0$ (i.e. $\mathbf{I}(G) = \mathbf{Z}G$ and $M = \lambda(M)$ for every M) or there exists a prime p such that T has exponent p or p^2 (and so the same is true for $M/\lambda(M)$). Note that if $T = 0$, then (4) splits as a sequence of G-modules (since $D = 1$). Thus S is a summand of a permutation lattice and is coflasque. In fact, one can show by a minor variation of the proof of Theorem 2.4 that for this collection of subgroups, S is always coflasque.

As in Section 2, the case of at most two subgroups is particularly nice. If there is only one subgroup, one can pass freely between the two approaches by taking duals. See (1) and (1′). We first record:

Lemma 3.5. *Let A be a ring (with 1). Let*

$$P \xrightarrow{f} Q \xrightarrow{g} R$$

be a complex of A-modules. If, for every A-module M, the induced complex of abelian groups

$$\mathrm{Hom}_A(R,M) \to \mathrm{Hom}_A(Q,M) \to \mathrm{Hom}_A(P,M)$$

is exact, then the original complex is an exact sequence.

Proof. Let M be any injective module containing $N = \ker(g)/f(P)$ (see [4, p. 9]). Assume that $N \neq 0$ (and so $M \neq 0$). Since M is injective there exists $h : Q \to M$ with $\ker(h) \cap \ker(g) = f(P)$. Thus $h \circ f = 0$, but $h \neq w \circ g$ for any $w \in \mathrm{Hom}_A(R,M)$ (since h does not vanish on all of $\ker(g)$). Thus the induced complex above with this M is not exact. □

We now show that for the case of two subgroups (11) has a very nice form. In particular, S' is torsionfree and the sequence is split exact as a sequence of abelian groups. Dualizing then yields a different (and perhaps easier) proof of Theorem 2.6. It is curious to note, however, that the dual approach does not seem to yield Theorem 2.4.

Theorem 3.6. *Let G be a finite group with subgroups C_1, C_2 and $D \subseteq C_1 \cap C_2$. Let $H = \langle C_1, C_2 \rangle$. The exact sequence (11) is now:*

$$0 \to T' \to \mathbf{Z}[G/D] \to \mathbf{Z}[G/C_1] \oplus \mathbf{Z}[G/C_2] \to \mathbf{Z}[G/H] \to 0. \tag{16}$$

In particular, S' is torsionfree.

Proof. We have the obvious complex of G-modules

$$\mathbf{Z}[G/D] \to \mathbf{Z}[G/C_1] \oplus \mathbf{Z}[G/C_2] \to \mathbf{Z}[G/H],$$

where the first maps send the class gD to (gC_1, gC_2) and the second map sends (aC_1, bC_2) to $aH - bH$. Note that the last map is obviously surjective.

For any G-module M, the induced sequence via $\mathrm{Hom}_G(\ ,M)$ is none other than

$$M^H \to M^{C_1} \oplus M^{C_2} \to M^D$$

with a suitable minus sign somewhere, and that sequence is obviously exact. It remains only to apply Lemma 3.5 to conclude that the sequence above is exact. All in all, this gives us the exact sequence (16) above (with the modification of a minus sign). □

We can also prove part of Proposition 2.5(a) from this approach. Simply start with the result of Theorem 2.6, and use $H^1(G, \mathbf{Z}[G/H] \otimes M) = 0$ if M is a permutation lattice. One then gets $M^D/(M^{C_1} + M^{C_2}) \subseteq \mathrm{Hom}_G(T', M)$, which shows the left-hand quotient is free.

4. The one subfield case

If A is a ring with 1, let A^* be its group of units. If K is any field, let $\mu(K)$ be the group of roots of unity in K. Let μ_n denote the group of nth roots of unity in an algebraic closure of K. Let $\mu_n(K)$ be the group of nth roots of unity in K.

We consider the structure of the torsion group of K^*/F^* for K a finite proper separable field extension of F. Let L be the Galois closure of K/F. Lemma 2.1, applied to the module L^* with G the Galois group of L/F, yields the following:

Proposition 4.1. *Let K/F be a finite separable extension of fields. Let L be the Galois closure of K/F.*

(a) *K^*/F^* embeds into a direct product of $[K : F] - 1$ copies of L^*.*

(b) *The n-torsion subgroup is finite for all n, and there is no p-torsion if K has positive characteristic p.*

(c) *If $\mu(L)$ is finite, then the torsion subgroup of K^*/F^* is finite.*

(d) *If F is finitely generated over the prime field, then the torsion subgroup of K^*/F^* is finite.*

Proof. If L is finitely generated over its prime field P, then so is any subfield. In particular, the subfield $P(\mu(L))$ is finitely generated and algebraic over P. This implies that $\mu(L)$ is finite (if the characteristic is positive, this subfield is finite; if the characteristic is zero, this follows from the fact that the degrees of the cyclotomic polynomials tend to infinity). This yields the last assertion in Proposition 4.1. □

It may happen that the torsion subgroup of K^*/F^* is infinite. By Proposition 4.1 this can happen only when $\mu(L)$ is infinite. In particular, if $K = \mathbf{C}$ and $F = \mathbf{R}$, then the torsion subgroup of K^*/F^* is infinite. We now construct another example. Let ℓ be a prime, and let $K = \mathbf{Q}(\ell^\infty)$ be the subfield of $\mathbf{C}$ generated by ℓ^d-th roots of 1

for all d. The automorphism group of K is the multiplicative group of units in the ℓ-adic integers (this is because the cyclotomic polynomials are irreducible over $\mathbf{Q}$). In particular, there exists an automorphism of order $\ell - 1$. If ℓ is odd, let F be the subfield fixed by this automorphism. Then F does not contain a root of unity of order ℓ. We conclude that the (infinite) ℓ-primary torsion subgroup of K^* injects into the ℓ-primary torsion subgroup of K^*/F^*. If $\ell = 2$, let F be the fixed field of complex conjugation. Then -1 is the only root of unity in F and the map from the 2-primary torsion subgroup of K^* to the 2-primary torsion subgroup of K^*/F^* has kernel of order 2. Again, K^*/F^* has an infinite 2-primary torsion subgroup. There are analogous examples with fields of positive characteristic.

We note that an example like the one above is impossible if l is odd and $\mu_\ell \subseteq F$ ($\mu_4 \subseteq F$ when $\ell = 2$):

Lemma 4.2. *Let L/F be a finite extension of fields of degree n. If ℓ is an odd prime and $\mu_\ell \subset F$, or if $\ell = 2$ and $\mu_4 \subset F$, then the ℓ-primary subgroup of $\mu(L)/\mu(F)$ is finite and has order dividing n.*

Proof. Let U be the ℓ-primary subgroup of $\mu(F)$ and V the ℓ-primary subgroup of $\mu(L)$. If U is infinite, then $U = V$ and the result holds. So assume U is finite. Let $\eta \in V - U$. It suffices to show that $\eta^n \in U$. Let m be the smallest power of ℓ such that $\eta^m \in U$. By hypothesis, $\eta^m \neq \pm 1$. It follows by [11, Theorem 51] that $x^m - \eta^m$ is irreducible over F. Thus $m|n$. □

Let G be a finite group of automorphisms of the field L. We need to know about the cohomology of the module $L^*/\mu(L)$. Since $H^1(G, L^*) = 0$ by Hilbert's Theorem 90, the long exact sequence for cohomology yields an injection:

$$0 \to H^1(G, L^*/\mu(L)) \to H^2(G, \mu(L)).$$

Lemma 4.3. *Let L be a field of characteristic $p \geq 0$. Assume G is a finite group of automorphisms of L.*

(a) *$H^1(G, L^*/\mu(L))$ is finite and its order is not divisible by p.*

(b) *For $i > 0$, $H^i(G, \mu(L))$ is finite and has order not divisible by p.*

(c) *$H^1(G, \mu(L))$ has order dividing $|G/D^2G|$.*

Proof. By the sequence preceding the lemma, (b) implies (a). We now prove (b). Let ℓ be a prime and let U_ℓ be the ℓ-primary component of $\mu(L)$. Let $\mathbf{Z}_\ell$ be the ring of ℓ-adic integers and $\mathbf{Q}_\ell$ its quotient field. If ℓ does not divide the order of G, then $H^i(G, U_\ell)$ is a $\mathbf{Z}_\ell$-module annihilated by $|G|$ and so is 0. If $p > 0$, then $U_p = 0$ and $H^i(G, U_p) = 0$. Since $\mu(L)$ is the direct sum of its primary subgroups, it suffices to prove that $H^i(G, U_\ell)$ is finite for each prime $\ell \neq p$ dividing the order of G. For each prime ℓ, the ℓ-primary component of $\mu(L)$ is either a finite (cyclic) group or is isomorphic (as abelian group) to the divisible group $\mathbf{Q}_\ell/\mathbf{Z}_\ell$. Since $H^i(G, M)$ is finite whenever M is a finitely generated G-module, we may assume that $U_\ell \cong \mathbf{Q}_\ell/\mathbf{Z}_\ell$.

Consider the exact sequence of $\mathbf{Z}_\ell G$-modules

$$1 \to \mathbf{Z}_\ell(1) \to \mathbf{Q}_\ell(1) \to \mathbf{Q}_\ell(1)/\mathbf{Z}_\ell(1) \to 1,$$

where $\mathbf{Z}_\ell(1)$ is the projective limit of the $\mathbf{Z}_\ell$-modules $\mu_{\ell^n}(L)$ (with respect to the ℓth power map), $\mathbf{Q}_\ell(1) = \mathbf{Q} \otimes \mathbf{Z}_\ell(1)$ and $\mathbf{Q}_\ell(1)/\mathbf{Z}_\ell(1)$ is the quotient, isomorphic to the group of ℓ-primary roots of 1. (All ℓ-primary roots of 1 are in L since we are assuming U_ℓ is infinite.) As a sequence of $\mathbf{Z}_\ell$-modules, this sequence is isomorphic to

$$0 \to \mathbf{Z}_\ell \to \mathbf{Q}_\ell \to \mathbf{Q}_\ell/\mathbf{Z}_\ell \to 0.$$

But for $i \geq 1$, $H^i(G, \mathbf{Q}_\ell(1)) = 0$ since this group is killed by the order of G and is also a $\mathbf{Q}_\ell$-vector space. Hence by the cohomology exact sequence

$$H^i(G, \mathbf{Q}_\ell(1)/\mathbf{Z}_\ell(1)) \cong H^{i+1}(G, \mathbf{Z}_\ell(1))$$

for $i \geq 1$, and the right-hand group is a finitely generated $\mathbf{Z}_\ell$-module killed by the order of G, hence finite.

Since $\mu(L)$ is locally cyclic, (c) follows by Lemma 2.12(b). □

The next result shows that infinite torsion in K^*/F^* occurs precisely because of roots of unity.

Theorem 4.4. *Let K/F be a finite proper separable extension of fields with Galois closure L. Let G be the Galois group of L/F.*

(a) *The natural injection $f : \mu(L)/\mu(F) \to (L^*/F^*)_{\text{tors}}$ has cokernel isomorphic to the finite group $H^1(G, \mu(L))$.*

(b) *The natural injection $h : \mu(K)/\mu(F) \to (K^*/F^*)_{\text{tors}}$ has finite cokernel isomorphic to a subgroup of the finite group $H^1(G, \mu(L))$.*

(c) *The torsion subgroup of K^*/F^* is finite if and only if $\mu(K)/\mu(F)$ is finite.*

(d) *If $\mu(K)$ is finite, then the torsion subgroup of K^*/F^* is finite. In particular, this is true if F is finitely generated over the prime field.*

Proof. (a) follows from Theorem 2.14(e) and Hilbert's Theorem 90. (b) follows from Theorem 2.14(d). Now (b) implies (c) and (d). □

Recall that a group G is called metabelian if $D^2G = 1$.

We now have:

Corollary 4.5. *Let K/F be a finite separable extension of fields. Let L be the Galois closure of K/F. Let $F_1 = F[\mu(K)]$ and F_2 be the maximal metabelian extension of F contained in L.*

(a) *If ℓ is an odd prime and $\mu_\ell \subset F$, then the ℓ-primary subgroup of K^*/F^* is finite and has order dividing $[F_1 : F][F_2 : F]$.*

(b) *If $\mu_4 \subset F$, then the 2-primary subgroup of K^*/F^* is finite and has order dividing $[F_1 : F][F_2 : F]$.*

Proof. Let ℓ be a prime and set U to be the ℓ-primary torsion subgroup of K^*. Note that $U \subset F_1$. If (a) holds with ℓ odd or (b) with $\ell = 2$, it follows by Lemma 4.2 that $U/(U \cap F^*)$ has order dividing $[F_1 : F]$. Theorem 4.4 asserts that the cokernel of the map $U/(U \cap F^*)$ into the ℓ-primary torsion subgroup of K^*/F^* has order dividing $|H^1(G, \mu(L))|$. By Lemma 4.3(c), this latter group has order dividing $[F_2 : F]$. This proves (a) and (b). □

Let K/F be as above. Brandis [2] proved that if K is infinite, then K^*/F^* is not finitely generated. Davis and Maroscia [5] proved that it has infinite torsionfree rank unless K is algebraic over a finite field or K/F is purely inseparable. One reduces very quickly to the case that K/F is a finite separable extension. See also [16] for results about embeddings of tori. As we mentioned in the introduction (see also 6.7 below), under this hypothesis the analogous result is true for two subfields as well, but not necessarily true for three. If $E_i, 1 \leq i \leq r$, are proper intermediate subfields of the finite separable extension K/F with K not algebraic over a finite field, then $K^*/E_1^*E_2^*$ has infinite torsionfree rank; but there are examples where $K^*/E_1^*E_2^*E_3^*$ is trivial [7, 1.11], finite but nontrivial (see Example 6.6 below), infinite torsion [7, Theorem 1.5] or of infinite torsionfree rank.

5. Two subfields

By Hilbert's Theorem 90, we know that if G is a finite group of automorphisms of the field L, then $H^1(G, L^*) = 0$. Thus Theorem 2.7 and Corollary 2.8 yield:

Theorem 5.1. *Let K/k be a finite separable extension of fields. Let E_1 and E_2 be intermediate fields with $F = E_1 \cap E_2$. Let L be the Galois closure of K/k.*

(a) *For each positive integer n, the n-torsion subgroup of $K^*/E_1^*E_2^*$ is finite and has order dividing $|\mu_n(L)|^s$, where $s = [K : F] + 1 - [E_1 : F] - [E_2 : F]$.*

(b) *If $\mu(L)$ is finite, then the torsion subgroup of $K^*/E_1^*E_2^*$ is finite.*

(c) *There is no p-torsion in $K^*/E_1^*E_2^*$ if k has positive characteristic p.*

(d) *If k is finitely generated over the prime field, then the torsion subgroup of $K^*/E_1^*E_2^*$ is finite.*

Proof. Let G be the Galois group of L/F. Let $C_i = \mathrm{Gal}(L/E_i)$ and $D = \mathrm{Gal}(L/K)$. Since $E_1 \cap E_2 = F$, $G = \langle C_1, C_2 \rangle$. We apply Corollary 2.8 (note $G = H$ in the notation of Corollary 2.8) to the G-module L^*. Since $H^1(G, L^*) = 0$, it follows that $K^*/E_1^*E_2^*$ embeds into $(L^*)^s$. Since $\mu_n(L)$ is cyclic and has no elements of order p if p is the characteristic of k, (a), (b) and (c) follow trivially. As for (d), it follows from (b) (since L is finitely generated over the prime field, $\mu(L)$ is finite). □

Wiegand [20, Corollary 2.4] proved the finiteness result for (a) when n is not a multiple of the characteristic. Holley [9] was the first to prove Theorem 5.1(b) and

(d) for n not divisible by the characteristic of k. Both Wiegand and Holley depend upon the finiteness of the n-torsion in Picard groups of curves [20, Theorem 2.1]. Their results give no information on the finiteness of the p-torsion when the field has positive characteristic p.

We can actually do a bit better than Theorem 5.1 in estimating the size of the torsion subgroup of $K^*/E_1^*E_2^*$.

Theorem 5.2. *Let K/k be a finite separable extension of fields. Let E_1 and E_2 be intermediate fields. Let L be the Galois closure of K/k and G the Galois group of L/k. Then the natural map*

$$\alpha : \mu(K)/\mu(E_1)\mu(E_2) \to (K^*/E_1^*E_2^*)_{\text{tors}}$$

has finite kernel and cokernel. The cokernel has exponent dividing $|G|^2$. The kernel is cyclic of order dividing $|H^1(G, \mu(L))|$. In particular, its order divides $|G/D^2G|$.

Proof. The fact that the cokernel has exponent dividing $|G|^2$ follows from Proposition 2.13 (see also 2.14 (a)) and from the fact that T is torsionfree. The finiteness of the cokernel follows from Lemma 4.3 and Theorem 2.14(c).

Now we prove that the kernel is finite. Let $F = E_1 \cap E_2$. If $x \in \mu(K)$ corresponds to an element of the kernel of α, then $x = yz$ with $y \in E_1$ and $z \in E_2$. Suppose $x^n = 1$. Thus $y^n = z^{-n} \in F$ and so y is a torsion element in E_1^*/F^* and z is a torsion element in E_2^*/F^*. By Theorem 4.4, the torsion subgroup of $(E_i^*/F^*\mu(E_i))$ has finite order d_i dividing $|H^1(G, \mu(L))|$. Let d be the least common multiple of the d_i. Then $y^d \in \mu(E_1)F^*$ and $z^d \in \mu(E_2)F^*$, and so $x^d = y^dz^d \in (\mu(E_1)\mu(E_2)F^*) \cap \mu(K) = \mu(E_1)\mu(E_2)$. Thus the kernel has finite exponent dividing $|H^1(G, \mu(L))|$, which divides $|G/D^2G|$ by Lemma 4.3(c).

The kernel is a subgroup of a homomorphic image of $\mu(K)$. Every finitely generated subgroup of $\mu(K)$ is cyclic and so the same is true for the kernel. Thus every finitely generated subgroup of the kernel is cyclic of order dividing d, and so the same is true for the entire kernel. □

Corollary 5.3. *Let K/k be a finite separable field extension. Let E_1 and E_2 be subfields of K each containing k.*

(a) *If $\mu(K)/\mu(E_1)\mu(E_2)$ is finite, then the torsion subgroup of $K^*/E_1^*E_2^*$ has finite order not divisible by the characteristic of k. In particular, this is true if k is finitely generated over the prime field.*

(b) *If k contains μ_ℓ (ℓ odd) or μ_4 ($\ell = 2$), then the ℓ-primary torsion subgroup of $K^*/E_1^*E_2^*$ is finite.*

Proof. The finiteness statement in (a) is an immediate consequence of the previous theorem. The fact that the order is not divisible by the characteristic of k follows from Theorem 5.1. Statement (b) follows from Theorem 5.2 and Lemma 4.2. □

A version of Theorem 5.1 holds in a more general situation. While Galois theory does not apply directly to (commutative) semisimple rings, it does to an extent that is sufficient for our purposes. Since the approach is so elementary, we include the next result. Most of it could be derived from the more general Galois theory of semiprime or artinian rings (cf. [12] and [15]). If K is a commutative finite-dimensional algebra over the field k, then K/k is separable if and only if K is a direct product of fields each of which is separable over k.

Proposition 5.4. *Let k be a field. Let K be a finite-dimensional separable k-algebra.*

(a) *There exists a finite-dimensional extension L of k containing K such that $L^G = k$, where $G = \mathrm{Aut}_k(L)$ with G finite.*

(b) *If E is a k-subalgebra of L, then there exists a subgroup C of G such that $L^C = E$.*

(c) *If H is a subgroup of G, then $H^1(H, L^*)$ is finite and its order is not divisible by the characteristic of k. Indeed, if we assume that H acts transitively on the primitive idempotents of L, then $H^1(H, L^*)$ is isomorphic to a subgroup of the abelianization of a subgroup of H.*

(d) *Let $\mu(L)$ denote the torsion subgroup of L^*. Then $H^1(H, L^*/\mu(L))$ is finite and its order is not divisible by the characteristic of k.*

Proof. Let $e_i, 1 \leq i \leq d$ be the primitive idempotents of K. Let $K_i = Ke_i$. We may assume that each K_i is contained in a given algebraic closure of k. Choose F a finite dimensional Galois extension of k containing each K_i. Set $L = Fe_1 \times \cdots \times Fe_d$. Then $G = \mathrm{Aut}_k(L) = \mathrm{Aut}_k(F) \wr S_d$ is finite and $L^G = k$. Thus (a) holds.

We now prove (b) by induction on d. If $d = 1$, the result follows by the Galois correspondence theorem. If E contains nontrivial idempotents, then L decomposes with respect to these idempotents and the result follows by induction. So we may assume that E is a field.

Since E is a field, it is isomorphic (over k) to its first projection E_1. Thus, there exist $\sigma_i \in \mathrm{Aut}_k(F)$ (with σ_1 the identity) such that

$$E = \{(\sigma_1(u), \ldots, \sigma_d(u)) : u \in E_1\}.$$

Let C be the subgroup of G fixing E pointwise. If $\rho \in G$ is any element acting via permutation of the coordinates and $\tau_i \in \mathrm{Aut}_k(F)$, then $\rho(\tau_1, \ldots, \tau_d)$ fixes E pointwise if and only if $\tau_{\rho(i)}\sigma_{\rho(i)} = \sigma_i$ on E_1.

Let E' be the subalgebra fixed pointwise by C. By the previous paragraph, C acts transitively on the set of primitive idempotents of L and so E' must be a field. Thus $E' \subseteq F' := \{(\sigma_1(u), \ldots, \sigma_d(u)) : u \in F\}$, which is k-isomorphic to F.

By the remarks above, the group J of automorphisms which stabilize F' induces the full group of automorphisms $\mathrm{Aut}_k(F')$ on F' and by the usual Galois correspondence, $C \cap J$ is trivial on no larger subfield of F' than E. Thus $E = E'$ as desired.

It remains only to prove the cohomology statements. Clearly, we may assume that H is transitive on the primitive idempotents of L. Let B be the subgroup of H stabilizing

a primitive idempotent e of L. Then $Le \cong F$ and L^* is isomorphic to the induced module $(F^*)_B^H$. Hence, by Shapiro's Lemma, $H^1(H,L^*) \cong H^1(B,F^*)$. Let A be the subgroup of B acting trivially on F. Since $H^1(B/A,F^*) = 0$ (by Hilbert's Theorem 90), it follows that $H^1(B,F^*)$ embeds into $\mathrm{Hom}_B(A,F^*) = \mathrm{Hom}_B(A,\mu(F))$. Since $\mu(F)$ is a locally cyclic group containing no elements of order equal to the characteristic of k, (c) follows.

Let $M = L^*/\mu(L)$. As above, $H^1(H,M) = H^1(B,F^*/\mu(F))$. Since $F^*/\mu(F)$ is torsionfree, it follows that $H^1(B,F^*/\mu(F)) \cong H^1(B/A,F^*/\mu(F))$. This latter group is a finite group whose order is not divisible by the characteristic of k by Lemma 4.3. □

If K/k is a finite-dimensional separable extension, a Galois closure of K/k is a separable finite-dimensional extension L/k such that $K \subseteq L$, $L^G = k$ for $G = \mathrm{Aut}_k(L)$, and no proper k-subalgebra of L satisfies those two conditions. Note that the previous result shows that Galois closures exist (and there is a uniqueness statement as well which we do not need). We can now apply the methods used to consider the field case. If K/k is a finite dimensional separable extension and E is an intermediate k-algebra, we can view E^* as the fixed points of a finite group G acting on L^*, where L is a Galois closure of K/k. This module has most of the properties as in the field case (in particular, although $H^1(G,L^*)$ need not be zero, it is still finite, the m-torsion subgroup of L^* is finite, every finitely generated subgroup of $\mu(L)$ is generated by at most d elements (where d is the number of primitive idempotents in K), and $H^1(G,L^*/\mu(L))$ is finite). These results, in conjunction with the proofs above, yield:

Theorem 5.5. *Let k be a field and K/k a finite-dimensional separable extension. Let E_1 and E_2 be k-subalgebras of K. Let J be the torsion subgroup of $K^*/E_1^*E_2^*$ and J_n the elements of J whose order divides n. Then*

(a) *J_n is finite.*
(b) *$J_p = 0$, if k has positive characteristic p.*
(c) *If $\mu(K)$ is finite, then J is finite.*
(d) *If k is finitely generated over the prime field, then J is finite.*
(e) *The natural map $\mu(K)/\mu(E_1)\mu(E_2) \to (K^*/E_1^*E_2^*)_{\mathrm{tors}}$ has finite cokernel.*

The example with $K = \mathbf{C} \times \mathbf{C}$ and k the diagonal shows that even over algebraically closed fields we cannot expect finite torsion in K^*/k^*.

If we replace the assumption of separability by semisimplicity (i.e., K is a finite-dimensional commutative k-algebra which is a direct product of fields), most of the previous results apply. Assume k has positive characteristic p. If F is a k-subalgebra of K, let F_s denote the subalgebra of k-separable elements of F. Note F^*/F_s^* is a p-group of finite exponent (because of the finite dimensionality). Then, $K_s^*/(E_1)_s^*(E_2)_s^*$ maps into $K^*/E_1^*E_2^*$. Since the group on the left has no elements of order p, it follows that this map is an embedding. The cokernel is a p-group of finite exponent. Thus $K^*/E_1^*E_2^*$ is the direct sum of a p-group of finite exponent and $K_s^*/(E_1)_s^*(E_2)_s^*$. This latter group satisfies the conclusions of Theorem 5.5. Thus:

Corollary 5.6. *Let k be a field of characteristic $p > 0$ and K/k a finite-dimensional semisimple commutative extension. Let E_1 and E_2 be k-subalgebras of K. Let J be the torsion subgroup of $K^*/E_1^*E_2^*$ and J_n the elements of J whose order divides n. Let $J_{p'}$ denote the subgroup of J consisting of elements whose order is not divisible by p. Then*

(a) *J_n is finite for n prime to p.*
(b) *The p-primary subgroup of J has finite exponent.*
(c) *If $\mu(K)$ is finite, then $J_{p'}$ is finite.*
(d) *If k is finitely generated over the prime field, then $J_{p'}$ is finite.*
(e) *The natural map $\mu(K)/\mu(E_1)\mu(E_2) \to J_{p'}$ has finite cokernel.*

6. Several subfields

If there are more than two subfields, we cannot say nearly as much. Applying Proposition 2.13 yields:

Theorem 6.1. *Let $E_i, 1 \leq i \leq r$, be intermediate fields for the finite separable field extension K/k. The cokernel of the natural map*

$$\mu(K)/\mu(E_1)\cdots\mu(E_r) \to (K^*/E_1^*\cdots E_r^*)_{\text{tors}}$$

has finite exponent.

The cokernel in the previous theorem can be infinite. See Example 6.4 below.

Corollary 6.2. *Let E_i, $i = 1,\ldots,r$ be intermediate fields for the finite separable extension K/k. Let ℓ be prime. Assume*

(i) *ℓ is odd and $\mu_\ell \subset k$,*
(ii) *$\ell = 2$ and $\mu_4 \subset k$, or*
(iii) *the ℓ-primary subgroup of $\mu(K)$ is finite.*

Then the ℓ-primary torsion subgroup of $K^*/E_1^*\cdots E_r^*$ has bounded exponent. In particular, this holds if k is finitely generated over the prime field.

Proof. This follows from Lemma 4.2 and Theorem 6.1. □

Let E_i, $i = 1,\ldots,r$ be intermediate fields for the finite separable extension K/k. Let L be the Galois closure of K/k with L/k of degree n. Then L embeds into $L \otimes_k L \cong L^n$ via $y \to 1 \otimes y$. Indeed, we can view $L \otimes_k L$ as a G-module where G acts trivially on the first factor and naturally on the second factor. Let $f : L \otimes_k L \to L \otimes \mathbf{Z}G$ be defined by $f(x \otimes y) = \Sigma_{g\in G} g(x)y \otimes g$. Note that f is a G-module map (where G acts diagonally on the right-hand side). Moreover, $L \otimes \mathbf{Z}G$ has an algebra structure (coordinatewise) and f is an algebra isomorphism. Thus f induces an isomorphism of $(L \otimes L)^*$ with $L^* \otimes \mathbf{Z}G$ with the diagonal action.

Restrict f to L^* (with the nontrivial action of G). So f injects L^* into $W := L^* \otimes \mathbf{Z}G$ via $y \to y \otimes N_G$, where $N_g = \Sigma_{g \in G} g$. This induces a homomorphism of abelian groups

$$\bar{f} : L^*/E_1^* \cdots E_r^* \to W/(W^{C_1} + \cdots + W^{C_r}).$$

If $r = 2$, then recall (Theorem 2.6) that in sequence (4), S is a permutation lattice and T is torsionfree. It follows easily from (10′) for both L^* and W and the fact that $H^1(G, L^* \otimes S) = H^1(G, W \otimes S) = 0$ that the kernel of $\bar{f}$ is 0.

If $r > 2$, we can apply Lemma 2.11. Thus, we have:

Proposition 6.3. *The map $\bar{f}$ defined above is an injection if $r \leq 2$. In general, the kernel of $\bar{f}$ has finite exponent dividing $|G|$.*

We now consider a modified version of the approach in [9]. Let K/k be a finite separable extension of fields with proper intermediate fields E_1 and E_2. Let P be a maximal ideal of $B = E_2[X]$ with $B/P \cong K$. Let A be the subring of B containing P with $A/P \cong E_1$. Then B is the normalization of A and P is the conductor of A. Since $\mathrm{Pic}(B)$ is trivial, it follows that $\mathrm{Pic}(A) = D(A) \cong K^*/E_1^* E_2^*$. Thus results about Picard groups can be applied to this group.

We may assume that k is a maximal subfield of A. Let L be the Galois closure of K/k and G the Galois group of L/k. Set $R = A \otimes_k L$. Then

$$\mathrm{Pic}(R) \cong (K \otimes_k L)^*/(E_1 \otimes_k L)^*(E_2 \otimes_k L)^*.$$

As in Section 6, we can identify these terms as the fixed points of certain subgroups of G where G is acting on $(L \otimes_k L)^*$. This last module is isomorphic to $L^* \otimes \mathbf{Z}G$ as a G-module. Thus, by Proposition 2.5(b), $\mathrm{Pic}(R)$ is isomorphic to a finite direct sum of copies of L^*. In particular, the n-torsion subgroup of $\mathrm{Pic}(R)$ is finite for all $n \geq 1$.

Let J be the kernel of the map from $\mathrm{Pic}(A)$ to $\mathrm{Pic}(R)$. It is straightforward to compute that J has exponent dividing $|G|$. If the order of G is not divisible by the characteristic of k, then [20, Theorem 2.1] applies and the kernel is finite. More generally, if m is not a multiple of the characteristic of k, [20, Theorem 2.1] implies that the m-torsion subgroup of J is finite. Thus, if m is not a multiple of the characteristic of k, the m-torsion subgroup of $\mathrm{Pic}(A)$ is finite.

However, we have seen (Proposition 6.3) that in fact J is trivial. This already yields an improvement of [9] – showing that there is no p-torsion in $\mathrm{Pic}(A) \cong K^*/E_1^* E_2^*$ and that the m-torsion subgroup is finite for all $m \geq 1$.

The finiteness of the kernel of $\bar{f}$ also is closely related to the question of whether or not S in the sequence (4) is coflasque. This is particularly evident for finitely generated fields (Theorem 7.2).

We now produce an explicit example with the kernel of $\bar{f}$ finite but nontrivial.

Example 6.4. Let L/k be a Galois extension of degree 4 with Galois group $G = \mathbf{Z}/2 \times \mathbf{Z}/2$. Let $E_i, 1 \leq i \leq 3$, be the three quadratic subfields. Let N be the norm map from L to k. Let $J = \ker(\bar{f})$.

(a) Then J maps onto $N(L^*) \cap L^{*2}/k^{*2}$. In particular, J may be nontrivial.

(b) If k is finitely generated over the prime field, then $L^*/E_1^*E_2^*E_3^*$ is an infinite group of exponent 2 and J is finite.

Proof. Let N_i be the norm map from E_i to k. If $x \in L^*$, then $f(x) = x \otimes N_G$. We can identify W with $L^* \otimes \mathbf{Z}G$ where G acts trivially on L^*, via $x \otimes g \to g^{-1}(x) \otimes g$. With this identification, $f(x) = \Sigma_g g^{-1}(x) \otimes g$. If $h \in G$, then

$$W^h = \left\{ \sum_g a_g \otimes g : a_{hg} = a_g \right\},$$

and so the product of coordinates of any element of $\lambda(W)$ is a square in L. Conversely, it is straightforward to see that if $w \in W$ has that property, then $w \in \lambda(W)$.

Thus $f(x) \in \lambda(W)$ if and only if $N(x)$ is a square in L. On the other hand, if $x \in E_1^*E_2^*E_3^*$, then, obviously, $N(x)$ is a square in k.

Let R be the subgroup of L^* consisting of those elements whose norm is a square in L. The previous paragraph shows that $J \cong R/E_1^*E_2^*E_3^*$ and that $N(\lambda(L^*)) \subseteq k^{*2}$. This proves the first assertion of (a).

Consider the special case $k = \mathbf{Q}$ and $L = \mathbf{Q}(i, \sqrt{2})$. If $x = 1 + i + \sqrt{2}$, $N(x) = 8$ is a square in L but not in k. Thus J is nontrivial. This completes the proof of (a).

(b) If $x \in L^*$, then $x^2N(x) = \prod_{1 \neq g \in G} xg(x) \in E_1^*E_2^*E_3^*$ and so $L^*/E_1^*E_2^*E_3^*$ is a group of exponent 2 and so certainly the kernel is as well. If L is finitely generated over the prime field, then the methods of the next section show that L^* is a direct sum of a finitely generated G-module and permutation lattices. It follows from Proposition 2.10 that in the case under discussion S (as in (4)) is a rank-two trivial G-module. It is straightforward (using the methods of Section 7, the structure of S and sequence (10′) for $M = L^*$ and $M = W$) to show that the kernel is finite.

We note that k is not an algebraic extension of a finite field since G is not cyclic. It follows from [7, (1.5)(c), (1.6), (1.8)] that $L^*/E_1^*E_2^*E_3^*$ is an infinite group of exponent 2. □

Using Example 2.9 and the methods of Section 7, we can produce fields where $\ker(\bar{f})$ is infinite.

Example 6.5. Let L/k be a Galois extension of number fields with Galois group G elementary abelian of order 8. Let $E_i, 1 \leq i \leq 3$ be intermediate fields with $[L : E_i] = 2$ and $k = E_1 \cap E_2 \cap E_3$. Then $\ker(\bar{f})$ is infinite.

Proof. As above, $\bar{f}$ maps $L^*/E_1^*E_2^*E_3^*$ to $L^* \otimes \mathbf{Z}G/\lambda(L^* \otimes \mathbf{Z}G)$. It is straightforward from the methods of Section 2 to show that the kernel of the map $\mathbf{Z}[G/H]/\lambda(\mathbf{Z}[G/H]) \to (\mathbf{Z}[G/H] \otimes \mathbf{Z}[G])/\lambda(\mathbf{Z}[G/H] \otimes \mathbf{Z}[G])$ is isomorphic to $H^1(H, S)$. By Example 2.9, there is a cyclic subgroup C of G with $H^1(C, S)$ nonzero. Since $\mathbf{Z}[G/C]$ occurs as a summand of L^* infinitely often (see Section 7), it follows that $\ker(\bar{f})$ is infinite. □

We next give an example with $K^*/E_1^*E_2^* \cdots E_r^*$ finite but nontrivial and K Galois over $k = E_1 \cap \cdots \cap E_r$. It follows from Section 7 below (proof of Theorem 7.2) that if K is finitely generated over the prime field, then the quotient being finitely generated implies that $T = 0$, whence the quotient is also trivial (under the assumption that K/k is Galois – see Corollary 2.3(g)). Al Sethuraman had suggested considering fields which are the intersection of a finite number of Henselizations.

Example 6.6. Let q be a prime. There exists a field k of arbitrary characteristic $p \neq q$ and a Galois extension K/k with Galois group $\mathbf{Z}/q \times \mathbf{Z}/q$ such that if $E_1, \ldots, E_r$ are all the intermediate extensions of K/k, then $K^*/E_1^* \cdots E_r^*$ is finite but nontrivial.

Proof. Let F be an algebraically closed field of characteristic p for any $p \neq q$. Let g_i be three distinct monic linear polynomials in $F[x]$. Let v_i be the corresponding valuation. Let F_i be a Henselization of $F(x)$ with respect to v_i. We also let v_i denote the extension of v_i to F_i. Set $k = F_1 \cap F_2 \cap F_3$. Let h_i be a qth root of g_i. Finally, set $K = F[h_2, h_3]$. Since $v_i(g_j) = \delta_{ij}$, it follows that K/k is a Galois extension with Galois group $G \cong \mathbf{Z}/q \times \mathbf{Z}/q$.

Also, since the residue field of the valuation ring of F_i is algebraically closed, it follows that any element t of F_i with $v_i(t)$ divisible by q is a qth power in F_i. Hence $t \in F$ is a qth power if and only $v_i(t)$ is divisible by q for each i. In particular $k^*/(k^*)^q$ has order q^3. It follows that $K^*/(K^*)^q$ is finite (this property is inherited by cyclic extensions of degree q – see [13, Corollary. 3.5, p. 203] for the case $q = 2$ – the proof given just above the corollary is valid for any prime).

Let $E_i, 1 \leq i \leq r$, be the set of extensions of k of degree q contained in K. It follows by [7, 1.6] that $(K^*)^q \subseteq E_1^* \cdots E_r^*$ and so $K^*/E_1^* \cdots E_r^*$ is finite.

Note that v_1 is unramified in K (since $v_1(g_2) = v_1(g_3) = 0$). Since the residue field is algebraically closed, this implies that v_1 splits completely from k to K. This yields a G-module surjection from K^* to $\mathbf{Z}G$ (defined by $x \mapsto (w_1(x), \ldots, w_{q^2}(x))$ where the w_i are the extensions of v_1). It follows from [7, 1.6] that $K^*/E_1^* \cdots E_r^*$ is nontrivial (or from the observation that T has order q for any noncyclic abelian q-group). □

We close this section with some remarks about the torsionfree rank of $K^*/E_1^* \cdots E_r^*$. These results are already in [7, Theorem 1.5]. Since there is no harm in replacing E_i by its purely inseparable closure in K, we may assume that K is separable over E_i.

Theorem 6.7. *Let K/k be a finite separable extension of fields. Let $E_1, \ldots E_r$ be proper intermediate subfields with $k = E_1 \cap \cdots \cap E_r$. Assume that K is not algebraic over a finite field. Then $\mathbf{Q} \otimes (K^*/E_1^* \cdots E_r^*) = 0$ if T is finite and has infinite dimension otherwise. In particular, if $r \leq 2$, $(K^*/E_1^* \cdots E_r^*)$ has infinite torsionfree rank.*

Proof. We apply Proposition 2.15 with $M = L^*$, L the Galois closure of K/k. The key observation is that $\mathbf{Q} \otimes L^*$ has a free $\mathbf{Q}G$ submodule of infinite rank (see [7, proof

of 1.5]; indeed the main result of [10] is that $\mathbf{Q} \otimes L^*$ is a free $\mathbf{Q}G$-module of rank equal to the cardinality of the field). If $r \leq 2$, then T is torsionfree of positive rank (by Theorem 2.6), hence infinite. □

7. Finitely generated fields

If k is finitely generated over the prime field, one can take a different approach. For the rest of this section, assume that k is such a field. Assume also that k is infinite. As usual K/k is a finite separable extension. Let L be the Galois closure.

Choose a domain A finitely generated over $\mathbf{Z}$ and with quotient field L. If E is an intermediate field, set $A_E = A \cap E$. Let E_i, $i = 1,\ldots,r$ be a collection of intermediate fields and set $A_i = A \cap E_i$. By inverting an element of A, we may assume that all A_i are regular. Classical and deep results due to Mordell, Weil, Severi and Néron imply (Roquette, see [14, Theorem. 6.6.2]) that $\mathrm{Pic}(A^C)$ is finitely generated for every subgroup C of G. So by inverting another element of A if necessary, we can assume that $\mathrm{Pic}(A^C) = 0$ for each subgroup C and that $A/(A \cap k)$ is unramified (i.e. the discriminant is a unit).

Then (since $\mathrm{Pic}(A) = 0$) we have the sequence

$$0 \to A^* \to L^* \to \Gamma \to 0,$$

where Γ is a direct sum of permutation lattices (corresponding to discrete rank-one valuations of L centered on height-one primes of A).

Since $\mathrm{Pic}(A^C) = 0$ and the extension A/A^C is unramified, $H^1(C, A^*) = 0$ for any subgroup C. Since Γ is a direct sum of permutation lattices, this implies that $\mathrm{Ext}^1_G(\Gamma, A^*) = 0$ and the sequence above is split exact as a sequence of G-modules. Thus

$$K^*/E_1^* \cdots E_r^* \cong (A \cap K)^*/A_1^* \cdots A_r^* \oplus \Gamma^D/(\Gamma^{C_1} + \cdots + \Gamma^{C_r}),$$

where C_i is the subgroup of G acting trivially on E_i.

Now assume that $r \leq 2$. Since Γ is a direct sum of permutation lattices, Proposition 2.5 implies that the torsion subgroup of $L^*/E_1^*E_2^*$ is isomorphic to the torsion subgroup of $A^*/A_1^*A_2^*$. Since A^* is finitely generated (see [14, 7.2, p. 42]) we have proved a weakened version of Corollary 5.3:

Theorem 7.1. *If k is a field finitely generated over the prime field, K is a finite separable extension field of k and E_1 and E_2 are proper subfields of K/k, then $K^*/E_1^*E_2^*$ is a direct sum of a countably generated free abelian group and a finite group. In particular, the torsion subgroup of $K^*/E_1^*E_2^*$ is finite.*

Note that this proof does not show that the p-torsion subgroup of $K^*/E_1^*E_2^*$ is trivial if k has positive characteristic p.

For general r, we see that $L^*/\lambda(L) \cong A^*/\lambda(A) \oplus \Gamma/\lambda(\Gamma)$. The left-hand term is finitely generated. The right-hand term essentially depends only on G and the C_i (and,

of course, the number of transitive permutation lattices of each type which are summands of Γ).

Theorem 7.2. *Let k be a field which is finitely generated over the prime field but is not algebraic over a finite field, K a finite separable extension field of k and $E_1,\dots,E_r$ proper subfields of K containing k. Let L be the Galois closure of K/k and G the Galois group of L/k. Let C_i be the Galois group of L/E_i. Define S and T as in* (4). *Then:*

(a) *If T is not torsionfree, $K^*/E_1^*\cdots E_r^*$ has infinite torsion subgroup (of finite exponent).*

(b) *If T is torsionfree, then $(K^*/E_1^*\cdots E_r^*)_{\mathrm{tors}} \cong Y \oplus H^1(G,\Gamma\otimes S)$, where Y is finite.*

(c) *If T is torsionfree and k is a number field, then*

$$(K^*/E_1^*\cdots E_r^*)_{\mathrm{tors}} \cong \bigoplus_{i=1}^{\infty}\left(\bigoplus_{C\in\mathscr{S}} H^1(C,S)\right)\oplus Y,$$

where Y is finite and $\mathscr{S}$ is the collection of all cyclic subgroups of G.

(d) *If T is torsionfree, $k = k_0(x)$, and $L = L_0(x)$ where k_0 is a subfield of k and L_0 is Galois over k_0, then*

$$(K^*/E_1^*\cdots E_r^*)_{\mathrm{tors}} \cong \bigoplus_{i=1}^{\infty}\left(\bigoplus_{C\in\mathscr{S}} H^1(C,S)\right)\oplus Y,$$

where Y is finite and $\mathscr{S}$ is the collection of all subgroups of G.

Proof. By [7, 1.8 and proof of 1.5], Γ has a $\mathbf{Z}G$-free direct summand of infinite rank. Thus Corollary 2.3(f) implies that $K^*/E_1^*\cdots E_r^*$ has a direct summand isomorphic to an infinite direct sum of copies of T. In particular, if T is not torsionfree, the torsion subgroup of $K^*/E_1^*\cdots E_r^*$ is infinite. It has finite exponent by Theorem 6.1. This proves (a). Since Γ is coflasque and torsionfree, (b) follows from Corollary 2.3(e).

If k is a number field, then since all residue fields are finite, the decomposition groups are cyclic (the extension A/A^G is unramified by the choice of A). The Chebotarev density theorem implies that each cyclic subgroup occurs as a decomposition group for infinitely many primes. Thus

$$\Gamma \cong \bigoplus_{i=1}^{\infty}\left(\bigoplus_{C\in\mathscr{S}} \mathbf{Z}[G/C]\right).$$

Corollary 2.3(f) implies (c).

(d) Under these hypotheses it follows that every subgroup of G will occur as a decomposition group infinitely often (e.g., consider the primes $x-a$ for various a in L). Now argue as in (c). □

The next result is an immediate consequence of Theorem 7.2.

Corollary 7.3. *Let G be a finite group with subgroups $C_1,\dots,C_r$ with $D\subseteq\bigcap_i C_i$. Let S and T be defined by* (4). *The following are equivalent:*

(a) *There exists no finite separable extension of fields K/k finitely generated over the prime field such that the Galois closure L/k has Galois group G and $K^*/E_1^* \cdots E_r^*$ has an infinite torsion group, where E_i is the fixed field of C_i.*

(b) *T is torsionfree and S is coflasque.*

The previous theorem allows us to give many examples in which T is torsion and so the torsion subgroup of $K^*/E_1^* \cdots E_r^*$ is infinite (see also [7, 1.4]). In particular, if G is a noncyclic p-group and $C_1, \ldots, C_r$ are the subgroups of index p, T will be an elementary abelian p-group (it is also easy to see in this case that S is a trivial G-module and so is coflasque).

Example 2.9 (see also 6.5) also shows that there are examples of number fields such that T is torsionfree and the torsion subgroup of $K^*/E_1^* \cdots E_r^*$ is infinite.

We do not know whether there exist examples of finitely generated fields such that $K^*/E_1^* \cdots E_r^*$ is finite but nontrivial. By Example 6.6, there are such examples without the finite generation restriction. It follows from the discussion preceding Theorem 7.2 that $K^*/E_1^* \cdots E_r^*$ finite implies that $T = 0$. If K/k is Galois, then it follows by Corollary 2.3(g) that $K^*/E_1^* \cdots E_r^*$ is trivial. So such an example could not be Galois. Moreover, $r \geq 3$ by Corollary 5.3.

The proof of Theorem 7.1 extends to the case when K is separable or semisimple (using the ideas in Theorem 5.5 and Corollary 5.6). Thus one has:

Theorem 7.4. *Let k be a field finitely generated over the prime field and K a finite dimensional semisimple commutative k-algebra. Let E_1 and E_2 be intermediate subalgebras of K/k.*

(a) *If k has positive characteristic p, then $K^*/E_1^*E_2^*$ is a direct sum of a countably generated free abelian group, a finite group and a p-group of finite exponent.*

(b) *If K/k is separable, then $K^*/E_1^*E_2^*$ is a direct sum of a countably generated free abelian group and a finite group.*

Acknowledgements

The second author would like to thank Al Weiss for some useful discussions.

References

[1] M. Aschbacher and R. Guralnick, Solvable generation of groups and Sylow subgroups of the lower central series, J. Algebra 77 (1982) 189–201.

[2] A. Brandis, Über die multiplikative Struktur von Körpererweiterungen, Math. Z. 87 (1965) 71–73.

[3] K. Brown, Cohomology of Groups, Graduate Texts in Mathematics, Vol. 87 (Springer, New York, 1982).

[4] H. Cartan and S. Eilenberg, Homological Algebra (Princeton University Press, Princeton, 1956)

[5] E. Davis and P. Maroscia, Affine curves on which every point is a set-theoretic complete intersection, J. Algebra 87 (1984) 113–135.

[6] R. Guralnick, D. Jaffe, W. Raskind and R. Wiegand, The kernel of the map on Picard groups induced by a faithfully flat homomorphism, J. Algebra, to appear.
[7] R. Guralnick and R. Wiegand, Galois groups and the multiplicative structure of field extensions, Trans. Amer. Math. Soc. 331 (1992) 563–584.
[8] W. Haboush, Multiplicative groups of Galois extensions, J. Algebra 165 (1994) 122–137.
[9] D. Holley and R. Wiegand, Torsion in quotients of the multiplicative group of a number field, in: R. Göbel, P. Hill and W. Liebert, eds., Abelian Group Theory and Related Topics, Oberwolfach, 1993, Contemp. Math. 171 (1994) 201–204.
[10] B. Jia, Splitting of rank one valuations, Comm. Algebra 19 (1991) 777–794.
[11] I. Kaplansky, Fields and Rings (University of Chicago Press, Chicago, 1972).
[12] V.K. Kharchenko, Automorphisms and Derivations of Associative Rings (Kluwer, Dordrecht, 1991).
[13] T.Y. Lam, The Algebraic Theory of Quadratic Forms (Benjamin, Reading, MA, 1973, 2nd print, 1980).
[14] S. Lang, Fundamentals of Diophantine Geometry (Springer, New York, 1983).
[15] T. Nakayama, Generalized Galois theory for rings with minimum condition, Amer. J. Math. 73 (1951) 1–12.
[16] Z. Reichstein and N. Vonessen, Torus actions on rings, J. Algebra 170 (1994) 781–804.
[17] P. Samuel, About Euclidean rings, J. Algebra 19 (1971) 282–301.
[18] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, Vol. 67 (Springer, New York, 1979).
[19] R. Wiegand, Picard groups of singular affine curves over a perfect field, Math. Z. 200 (1989) 301–311.
[20] R. Wiegand, Torsion in Picard groups of affine rings, in: W. Heinzer, C. Humeke and J. Sally, eds., Commutative Algebra: Syzygies, Multiplicities and Birational Algebra, Mount Holyoke College, 1992, Contemp. Math. 159 (1994) 433–444.